



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/981,470	10/16/2001	Roberto J. Pimentel	09469.013001; 97.0011	5937

22511 7590 04/11/2005

OSHA & MAY L.L.P.  
1221 MCKINNEY STREET  
SUITE 2800  
HOUSTON, TX 77010

EXAMINER
----------

POLTORAK, PIOTR

ART UNIT	PAPER NUMBER
----------	--------------

2134

DATE MAILED: 04/11/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/981,470	<b>Applicant(s)</b> PIMENTEL ET AL.	
	<b>Examiner</b> Peter Poltorak	<b>Art Unit</b> 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 1-23-2002.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-61 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-61 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

### DETAILED ACTION

1. Claims 1-61 have been examined.
2. The effective filing date for the subject matter defined in the pending claims in this application is 10/16/2001.

### ***Claim Rejections - 35 USC § 112***

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 5-6, 33-34 and 48-49 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention.
4. The specification provides no guidance in teaching how the embedding of Public Key Infrastructure mechanism between the client stack and the client-side application adapter is achieved and as a result it does not allow to determine how the client stack and data is encrypted using a Public Key Infrastructure mechanism embedded between the client stack and the client-side application adapter.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Art Unit: 2134

5. Claims 1-61 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that applicant regards as the invention.
6. Claims 1, 3, 16-17, 20, 30-31, 44-46, 50 and 59-61 recite the phrase "between the wireless client and the enterprise server". It is not clear whether the term limits the occurrence of the event (e.g. encryption) to take place somewhere on the path from the wireless client to the enterprise server or whether the event must start at the wireless client and must complete at the enterprise server. For purposes of further examination an event taking place at the path between the client and the server is treated as meeting the claim limitations.
7. Claims 7 and 18 recite: "the server stack is Wireless Application Protocol compliant". The limitation is not understood. The specification points out that the enterprise server is not a WAP-compliant server and that it relies on the WAP compliant server stack to manage sessions, transaction, and datagram transport services. No other details of the "compliance" (as used in the limitation) and what it stands for is provided. The limitation is especially puzzling since the server stack is implemented (located) within the enterprise server, and it is unclear how the entity could not be WAP-compliant if one of the entity's parts was WAP-compliant.
8. Claim 30 recites the terms: "authentication information" in line 10, 11 and 13. It is not clear whether all of the terms are unrelated. For example line 10 first recites that the authentication information is requested from an authentication

manager module, then line 11 continues that (*the?*) authentication information is checked in a volatile memory, followed by line 13 stating that (*the?*) authentication information is authenticated on the enterprise server.

However, none of these terms have preceding articles that suggests none of these terms is related to each other.

Furthermore, the dependent claims 41 and 42 recite the terms: "the authentication information" which further makes the issue more ambiguous. It is not clear to which of the above authentications the terms refer.

A similar problem is observed in claims 44-45, 56-57 and 59-61.

The claims are addressed as best understood.

9. Claims 15, 27, 39 and 54 recite a remotely configurable time limit of volatile memory within the authentication manager module. It is unclear whether the limitation refers to clients, which are to be authenticated, whether the authenticating entity is a distributed entity containing the authentication manager module and the memory in two remote locations or whether there is some other interpretation of the claim limitation. The claim is treated as best understood.

10. Claims 2, 4-6, 8-14, 19, 21-26, 28-29, 33-38, 40-43, 47-49, 51-53 and 55 are rejected by virtue of their dependence.

Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

11. Claims 1-4, 7-8, 11, 16-21, 23 and 28 are rejected under 35 U.S.C. 102(b) as being anticipated by *Jormalainen et al.* (Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999).

12. As per claims 1-2, 7-8, 11, 16-18, 20-21 and 23 (as best understood) *Jormalainen et al.* teach Wireless Transport Layer Security (WTLS), wherein a wireless client communicates with a server using a wireless (WAP) gateway (Fig. 3.1).

The wireless gateway translates requests from the WAP protocol stack to the Internet protocol stack (TCP/IP). The Wireless Session Protocol (WSP) provides ways to establish a session from client to server (3.1 "Overview of The Wireless Application Protocol" section including Fig. 3.1 and Fig. 3.2).

The TCP/IP implemented (*located*) on the server reads on the server stack and the WAP implemented (*located*) on the client reads on a client stack.

Both stacks provide communication services between the enterprise server and the wireless client.

As well known in the art, Application Program Interfaces (API) define the way that application programs interact with protocol stacks and as such they read on interface, a server-side application adapter providing an interface between the server stack and a server application located on the enterprise server and a client-side application adapter providing an interface between the client stack and a client application located on the wireless client.

*Jormalainen et al.* also teach authentication between the client and the server, an explicit verification carried out by the client, wherein the client concatenates all the messages received from the server or created by itself and calculates a hash value to be signed. This message is sent to the server, which can ensure that authentication has gone well so far (3.4

*"Authentication" section*).

The module responsible for authentication reads (and other security related functions) on an authentication manager module managing authentication information in the volatile memory and transferring authentication information to the client-side application adapter. The wireless client inherently stores authentication information in the memory.

13. As per claims 19 and 28 interrupt signals used within computing devices to indicate occurrence of particular application events read on the specific business logic.

As per claims 3-4 *Jormalainen et al.* (as best understood) teach that encrypting data transferred between the client and the wireless gateway is encrypted using WTLS that is embedded within the client stack (*Fig. 3.2 and 3.2 "Specification" section*) and use X.509 certificates (*authentication*).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to

be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. Claims 30-32, 35, 45-47, 50 and 60-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) in view of *Stein* (*Lincoln D. Stein, "Web Security, a step-by -step reference guide", 1998, ISBN: 0201634899*).
15. *Jormalainen et al.* teach the wireless client, receiving data on the enterprise server and sending a request from the client stack to the enterprise server as discussed above. Furthermore, *Jormalainen et al.* teach a gateway providing an interface between the enterprise server and the wireless client (Fig. 3.1), a secure session between the wireless client and the enterprise server (Fig. 3.5, 3.3.3 "The Handshake Protocol" section and 3.8 "Secure State" section). When an application on the enterprise server sends a notification message (or any data) to the wireless client the notification message will inherently go through the server-side application adapter (API) (after triggering an event) and the server stack before ends up at the client. At the client side the incoming message inherently travels in the reversed order.
16. *Jormalainen et al.* do not teach enterprise server authenticating authentication information on the enterprise server.
17. *Stein* teach enterprise sever authenticating authentication information on the enterprise server (*pg. 41 including Fig. 32*).
18. It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to include enterprise sever authenticating authentication



Art Unit: 2134

information on the enterprise server as taught by *Stein* in *Jormalainen et al.*'s invention. One of ordinary skill in the art would have been motivated to perform such a modification in order to authenticate the client.

19. Claims 9 and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) in view of *Official Notice*.

20. *Jormalainen et al.* teach the volatile memory as discussed above.

*Jormalainen et al.* do not explicitly teach that the volatile memory is Random Access Memory (RAM).

21. *Official Notice* is taken that it is old and well-known practice to use RAM as volatile memory. One of ordinary skill in art at the time of applicant's invention would employ RAM to take advantage of the low price of well-known and proven technology.

22. Claims 43 and 58 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) in view of *Stein* (*Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899*) and in further view of *Official Notice*.

23. Claims 43 and 58 add limitations substantially equivalent to claims 9 and 22; therefore claims 43 and 58 are similarly rejected.

24. Claims 10 and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the*

Art Unit: 2134

*WTLS, 30/11/1999) in view of RFC 2614 (RFC2614, J. Kempf, E. Guttman, "An API for Service Location", June 1999).*

25. *Jormalainen et al.* teach the client-side application adapter as discussed above. As per claims 10 and 29 *Jormalainen et al.* do not explicitly teach configuring the application adapter using a configuration file.
26. *RFC 2614* teach configuring the application adapter using a configuration file (*RFC 2614, Abstract*). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to configure the application adapter using a configuration file as disclosed in *RFC 2614*. One of ordinary skill in the art would have been motivated to perform such a modification in order to set parameters in a portable way (*RFC 2614, Abstract*).
27. Claims 40 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999) in view of Stein (Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899) and in further view of RFC 2614 (RFC2614, J. Kempf, E. Guttman, "An API for Service Location", June 1999).*
28. Claims 40 and 55 add limitations substantially equivalent to claims 10 and 29; therefore claims 40 and 55 are similarly rejected.
29. Claims 12-14 and 24-26 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999) in view of Pfeiffer et al. (U.S. Patent No. 5535366).*

Art Unit: 2134

30. *Jormalainen et al.* teach the authentication manager module and the volatile memory as discussed above.
31. *Jormalainen et al.* do not teach authentication manager module controlling a configurable time limit of volatile memory that is erased when the time limit is reached.
32. *Pfeiffer et al.* teach a configurable time limit of volatile memory that is erased when the time limit is reached (*Pfeiffer et al., Abstract*). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to extend the authentication manager module as taught by *Jormalainen et al.* to control configurable time limit of the volatile memory that is erased when the time limit is reached as taught by *Pfeiffer et al.* One of ordinary skill in the art would have been motivated to perform such a modification in order to avoid permanent blockage of the memory (*Pfeiffer et al., Abstract*) and in order to increase security (e.g. to prevent buffer overflow attacks).
33. Claims 36-38, 44, 51-53 and 59 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) in view of *Stein (Lincoln D. Stein, "Web Security, a step-by -step reference guide", 1998, ISBN: 0201634899)* and in further view of *Pfeiffer et al. (U.S. Patent No. 5535366)*.
34. Claims 36-38 and 51-53 add limitations substantially equivalent to claims 12-14 and 24-26; therefore claims 36-38 and 51-53 are similarly rejected.
35. Claims 44 and 59 are substantially equivalent to claims 36 and 51; therefore claims 44 and 59 are similarly rejected.

Art Unit: 2134

36. Claims 15 and 27 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) in view of *Pfeiffer et al.* (*U.S. Patent No. 5535366*) and in further view of *Krishnamurthy et al.* (*U.S. Patent No. 6389464*).
37. *Jormalainen et al.* in view of *Pfeiffer et al.* teach the time limit configurable from within the authentication manager module. *Jormalainen et al.* in view of *Pfeiffer et al.* do not teach that the time limit is remotely configurable. *Krishnamurthy et al.* teach a remote configuration and provides a motivation to combine by stating benefits of the remote configuration (*Krishnamurthy et al., col. 18 lines 14-27*).
38. Claims 39 and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) and *Stein* (*Lincoln D. Stein, "Web Sercurity, a step-by - step reference guide", 1998, ISBN: 0201634899*) in view of *Pfeiffer et al.* (*U.S. Patent No. 5535366*) and in further view of *Krishnamurthy et al.* (*U.S. Patent No. 6389464*).
39. Claims 39 and 54 add limitations substantially equivalent to claims 15 and 27; therefore claims 39 and 54 are similarly rejected.
40. Claims 41 and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) in view of *Stein* (*Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899*) and in further view of *Official Notice*.

Art Unit: 2134

41. *Jormalainen et al.* in view of *Stein* teach the authentication as discussed above.

*Jormalainen et al.* in view of *Stein* do not explicitly teach that the authentication information comprises a username and a password.

*Official Notice* is taken that it is old and well-known practice to use a username and a password as authentication information. One of ordinary skill in art at the time of applicant's invention would use a user username and a password as authentication information in order to assure that the user accesses only information authorized for this user.

42. Claim 42 and 57 are rejected under 35 U.S.C. 103(a) as being unpatentable over *Jormalainen et al.* (*Sami Jormalainen and Jouni Laine, "Security in the WTLS, 30/11/1999*) in view of *Stein* (*Lincoln D. Stein, "Web Sercurity, a step-by -step reference guide", 1998, ISBN: 0201634899*) and in further view of *Orgam* (*U.S. Patent No. 6085324*).

43. *Jormalainen et al.* in view of *Stein* teach a wireless client and the authentication as discussed above.

*Jormalainen et al.* in view of *Stein* do not explicitly teach that the authentication information comprises a wireless client address and a password.

*Ogram* teaches the authentication information that comprises an address and a password (*Ogram, col. 7 lines 18-20*).

It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to use the authentication information that comprises a

Art Unit: 2134


wireless client address and password address and a password as taught by *Ogram*. One of ordinary skill in the art would have been motivated to use the authentication information that comprises an address and a password in order to authenticate a valid user.


### **Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571)272-3840. The examiner can normally be reached Monday through Thursday from 9:00 a.m. to 4:00 p.m. and alternate Fridays from 9:00 a.m. to 3:30 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
3/30/05

  
GREGORY MORSE  
SUPERVISOR, EXAMINER  
TECHNICAL CENTER 20